UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

Joint Stock Company "Channel One Russia Worldwide," Closed Joint Stock Company "CTC Network," Closed Joint Stock Company "TV DARIAL," Closed Joint Stock Company "New Channel", Limited Liability Company "Rain TV-Channel,", and Limited Liability Company "Global Entertainment TV."

Index No. 16-cv-1318 (GBD)(BCM)

Plaintiffs,

-against-

DECLARATION OF DMITRI DIETRICH IN OPPOSITION TO SANCTIONS

INFOMIR LLC (www.infomirusa.com), INFOMIR GMBH, ALEXANDER MARAHOVSKY, EVGENI LEVITIN, TELETRANSFERS TECHNOLOGIES LTD., PANORAMA ALLIANCE, LP (www.mypanorama.tv), ASAF YEVDAYEV, DAVID ZELTSER, S.K. MANAGEMENT OF NEW YORK, INC. (www.gudzon.tv), MOIDOM LLC, TELEPROM, VDALI, MHCOM GmbH and John Does 1-50.

Defendants.

----------X

DMITRI DIETRICH declares subject to penalty of perjury under the laws of the United States of America as follows:

1. I am over the age of eighteen, of sound mind and otherwise competent to make this Affidavit, not a party to this action, and the Chief Technical Officer of Kartina Digital GmbH ("Kartina"), Rheingaustr. 53, 65201 Wiesbaden, Germany.

2. I am able to read and write in English.

3. I have worked at Kartina for nearly twelve (12) years.

4. I received a degree in "informatik" or computer science from Fachhochschule Wiesbaden in 2006 and am familiar with, among other things, internet protocol television ("IPTV").

5. I have reviewed a November 3, 2018 report by Christopher Rucinski, Vice President at Stroz Friedberg ("Rucinski Report" or "Ruc. Rep.") (ECF 694-1), criticizing Christopher Vidulich's Affidavit dated June 24, 2016 ("Vidulich Affidavit" or "Vid. Aff.") (ECF 80) and purporting to raise questions regarding the May 24, 2016 Wireshark capture file entitled "Channel_One_Capture.pcapng" Bates No. CHANNELONE003307 ("Channel One PCAP").

6. I also reviewed the November 21, 2018 Affidavit, from Akbar A. Khan ("Khan Affidavit" or "Khan Aff.") containing webpages, screenshots, and coding from Mr. Khan's investigation of various web pages, set-top boxes ("STBs"), and software development kits ("SDKs"). I am personally familiar with the sources referenced in the Khan Affidavit.

7. As explained in the Rucinski Report, Wireshark is a software program that allows a user to record data transmission across computer networks by capturing data in a file. (Ruc. Rep. at 2-3). The file format in which Wireshark stores captured data is the "PCAP" format with file extension ".pcap" or ".pcapng." (*Id.*) The Channel One PCAP is saved with the file extension ".pcapng" indicating that the file is a PCAP file and can therefore be opened and analyzed on Wireshark.

8. An STB is a device that receives video data through the internet, by, for example, connecting to a radio wireless local area network, referred to herein as "Wi-Fi," and converts the data it receives into video streaming capable of being displayed on a television screen or display device.

I. Evidence from the Channel One PCAP and Vidulich Affidavit Was Not Lost or Spoliated and this is Confirmed by the Rucinski Report

9. I am informed that the Rucinski Report was submitted to support Infomir's allegations that electronically stored information was lost or destroyed. As explained below, the Rucinski Report makes no such allegation and Infomir's assertion is wrong.

10. Nothing in the Rucinski Report or from my knowledge of our investigation into Infomir's piracy suggests that data or evidence from the Channel One PCAP was lost or spoliated by Dunnington Bartholow Miller LLP ("Dunnington") or Plaintiffs. To the contrary, Mr. Rucinski's inspection of the Channel One PCAP and his findings about it confirm that the Channel One PCAP was not lost and was produced to Defendants.

11. In addition, I see nothing in the either the Channel One PCAP or the Rucinski Report to suggest that Dunnington or Plaintiffs destroyed or tampered with evidence and I do not believe this to be the case. Mr. Rucinski confirms that the Channel One PCAP is a single Wireshark capture on May 24, 2016 (Ruc. Rep. at 4) and does not point to any evidence of spoliation or tampering with the ".pcap" file.

12. To the extent that Mr. Rucinski suggests that Dunnington withheld the Channel One PCAP to present difficulties to Infomir, the circumstances suggest otherwise. As explained in more detail below, Infomir could have run tests on its servers to monitor activity on May 24, 2016 to easily rebut any false allegations of IPTV streaming.

13. Dunnington's production of screenshots, PDFs, and XPSs of the Wireshark capture instead of sending the capture file itself, caused no prejudice to Infomir because Infomir should be in possession of evidence of its streaming activities, or lack thereof.

II. The Vidulich Affidavit Accurately Shows that the Aura HD STB was Connected to Wi-Fi and that Video Data Transfer Between the Aura HD STB and Infomir Stalker Occurred While Mr. Vidulich Observed Pirated Programming

A. The Vidulich Affidavit Accurately Shows the Aura HD STB was Connected to Wi-Fi via a Laptop Bridge

14. The Rucinski Report argues that an optional Wi-Fi adapter plug-in is the only method to connect the Aura HD STB to Wi-Fi. (Ruc. Rep. at 13). Based on this, the Rucinski Report concludes that Mr. Vidulich's explanation that the Aura HD STB was connected to the

internet through Wi-Fi is "technologically impossible" (Ruc. Rep. at 4).

15. Mr. Rucinski's arguments and conclusions are erroneous. A Wi-Fi adapter plugin is not the only method for connecting the Aura HD STB to Wi-Fi.

16. One can use a wireless-enabled laptop as a bridge to connect an Aura STB to the internet by running an Ethernet cable from the STB to the laptop. A "bridge connection" allows a user to monitor and record the traffic capture file (.pcap) between the laptop's Wi-Fi connection and laptop's Ethernet port (a physical connection to the Aura HD STB).

17. The bridge connection method connects a STB to a laptop with an Ethernet cable and then connects the laptop to Wi-Fi, which in turn connects the STB to the internet. We refer to the laptop as a "bridge" to the internet because it serves as the channel through which the STB accesses the internet.

18. The hardware setup described and depicted in the photograph attached to the Vidulich Affidavit shows the bridge method of connecting the Aura HD STB to Wi-Fi. (Vid. Aff. Ex. 6). The photograph shows that the Aura HD STB uses a Dell laptop as a bridge because the STB is connected to the laptop through an Ethernet cable. (Vid. Aff. Ex. 6).

19. By using the Dell laptop as a bridge, as the photograph shows, Mr. Vidulich was able to connect the Aura HD STB to the internet because the laptop was connected to Wi-Fi, in turn connecting the STB to Wi-Fi. (Vid. Aff. Ex. 6).

20. Mr. Rucinski's conclusions should be rejected. His report does not appear to have examined the photograph attached as Exhibit 6 to the Vidulich Affidavit.

21. I can confirm that Mr. Vidulich used the bridge method based on personal knowledge because I have done this myself and I guided Mr. Vidulich on how to configure the hardware to connect the Aura HD STB to the Internet with the Dunnington firm's Dell laptop.

22. I instructed him to connect the Aura HD STB to the Dell laptop with an Ethernet cable and the laptop to the Internet through a Wi-Fi connection. (Vid. Aff. Ex. 6).

23. Additionally, Mr. Rucinski's conclusion that the STB could not connect to the internet is faulty because it is contradicted by evidence in the PCAP showing the Dell laptop connecting to the internet.

24. The Channel One PCAP itself is consistent with the Aura HD STB connecting to the Internet via the Dell laptop's Wi-Fi connection. Exhibit 1 hereto is a screenshot of the Channel One PCAP. In the Channel One PCAP, one can see in packet 1 under the "Ethernet II" tab, the following language: "Address: Dell_67:34:b6 (5c:26:0a:34:b6)" ("Dell Address"). The Dell Address language is highlighted by the red marking "NOTEBOOK." (Ex. 1).

25. The Dell Address is the Dell laptop's unique Media Access Control ("MAC") address. A MAC address is an identifying number for a physical device that is hardwired or hard-coded into the device's hardware to create a digital footprint that can allow one to identify the source of data activity on the internet. The Dell laptop's MAC address appears in any data packet sent to and from the Aura HD STB because the Dell laptop is used as a bridge.

26. The Dell Address in the Channel One PCAP file signifies that the source MAC address for packet 1 is from the Dell laptop photographed in Exhibit 6 of the Vidulich Affidavit, thus confirming Vidulich's testimony. (Ex. 1).

27. The Channel One PCAP contains additional evidence contradicting Mr. Rucinski's conclusion that the Aura HD STB could not have connected to the internet via Wi-Fi.

28. The Channel One PCAP shows that both the laptop and the Aura HD STB were connected to Wi-Fi when the Wireshark capture occurred because the Aura HD STB was both sending and receiving data to and from sources that the STB could not have connected to without

Wi-Fi, such as Infomir's servers.

29. This can be seen at Exhibit 2, a screenshot of the Channel One PCAP depicting packet 12. In contrast to packet 1 where the Dell laptop was the source of the data transfer, packet 12 shows that the Dell laptop's MAC address is the recipient of data because the same MAC address, "Dell_67:34:b6 (5c:26:0a:34:b6)," is the destination address. (*Compare* Ex. 1, *with* Ex. 2).

30. If the Aura HD STB was not connected to the internet as Mr. Rucinski suggests, the only data transfers one would see in a Wireshark capture would be to and from devices physically connected to the Aura HD STB.

31. In this case, the only device physically connected to the Aura HD STB through an Ethernet cable was the Dell laptop photographed in Exhibit 6 to the Vidulich Affidavit. (Vid. Aff. Ex. 6).

32. If the Aura HD STB had not been connected to the internet, we would only see data transfers between the Dell laptop and the Aura HD STB. The Channel One PCAP, however, shows data transfers from more than just two devices, including Infomir's servers, which is only possible if the Aura HD STB is connected to the internet and able to communicate with sources, like Infomir's servers, beyond those physically connected to it.

33. Based on the foregoing, I find that Mr. Rucinski was incorrect in concluding that Dunnington's hardware setup made it impossible to connect the Aura HD STB to the internet via Wi-Fi. (Ruc. Rep. at 5). Dunnington's hardware setup allowed the Aura HD STB to connect to the internet by using the Dell laptop as a bridge to Wi-Fi. My review of the Channel One PCAP confirms that the Aura HD STB was in fact connected to internet while Mr. Vidulich viewed pirated broadcasts.

B. The Rucinski Report Concedes that a Wireshark Capture Occurred on May 24, 2016 and that Such Capture Reveals Data Transfers Between the Aura HD STB and Infomir Stalker

34. My review of the Channel One PCAP on Wireshark confirms Mr. Rucinski's conclusion that a Wireshark capture occurred on May 24. 2016.

35. Under the "Statistics" tab in Wireshark, one can examine the Channel One PCAP by clicking on "Capture File Properties" to open a window that provides information about Channel One PCAP like the number of packets captured, how long the capture lasted, and on what date the capture occurred.

36. From this examination, we can see that the first and last data packet were captured on May 24, 2016 confirming that the date of the Channel One PCAP was May 24, 2016.

37. Furthermore, my review of the Channel One PCAP shows that on May 24, 2016, the Aura HD STB had data transfers with Infomir's Stalker Middleware, a product downloadable from the Infomir website. (Khan Aff. at 5).

38. Data transfers with Infomir's Stalker Middleware are indicated in the Wireshark capture by the presence of the Aura HD STB IP address as both the source and destination IP address for various data transfers to and from the "stalker_portal" domain. The occurrence of such data transfers is consistent with Vidulich's eyewitness testimony of observing pirated broadcasts during the Wireshark capture. (Vid. Aff. at 4-5).

39. Mr. Rucinski fails to address data transfers between Stalker Middleware and the Aura HD STB and instead limits his discussion to data transfers between the domain "freetvstat.iptv.infomir.com.ua" and the Aura HD STB. (Ruc. Rep. 11-13). Although Rucinski doesn't say so, the presence of "Infomir" in the domain name indicates that this domain belongs to or is related to Infomir.

40. Mr. Rucinski concedes the occurrence of data transfers between the Aura HD STB and "freetvstat.iptv.infomir.com.ua" when he investigates the exchange of data packets between Aura HD STB and "freetvstat.iptv.infomir.com.ua. (Ruc. Rep. 11-13). Although Mr. Rucinski suggests that Mr. Vidulich's Affidavit does not show video data transfers (Ruc. Rep. at 4), his report concedes that the Channel One PCAP reflects video data transfers. His report, however, does not explain the content or source of the video data transfers in the Channel One PCAP. As discussed below, my analysis of the Channel One PCAP data shows that the video data is consistent with Infomir video streaming pirated IPTV broadcasts.

41. As the Rucinski Report correctly identifies, the Aura HD STB IP address is "192.168.12.136." To confirm this, while accessing the Channel One PCAP, one can open a data packet in Wireshark in which "192.168.12.136" is listed as the source IP address.

42. In such a packet, for example, packet 12, the "User-Agent" field under "Hypertext Transfer Protocol," states "MAG200," indicating that the source IP address for this data packet was coming from an STB. Attached hereto as Exhibit 3 is a screenshot of packet 12's data transfers. The "MAG200" language is indicated with a red line.

43. Given that the only STB box connected to Wi-Fi was the Aura HD STB pictured in Exhibit 6 of the Vidulich Affidavit, I conclude that the IP address for the Aura HD STB is "192.168.12.136."

44. Once we identify "192.168.12.136" as the Aura HD STB's IP address, we can isolate all data coming into and out of the box during the Channel One PCAP by typing the following command in the text box of the Wireshark program: "ip.dst==192.168.12.136 or ip.src==192.168.12.136."

45. This command isolates all data packets in which either the source or destination IP

address was "192.168.12.136," or the Aura HD STB's IP address.

46. One can further refine the Wireshark analysis of the Channel One PCAP by grouping specific types of transfers, for example, transfers involving HTTP data, together. To do this, one clicks on the "Protocol" column in Wireshark and scrolls down to the data packets with "HTTP" protocols. Through this process of IP address isolation and protocol reorganization, one can isolate all HTTP data transfers going into and out of the Aura HD STB at the time of the Channel One PCAP Wireshark capture.

47. Reviewing the HTTP data transfers occurring during the Channel One PCAP capture, I see data communications exchanged between Stalker Middleware and the Aura HD STB. For example, packet 87 (a screenshot of which is attached hereto as Exhibit 4) contains data transfers from the Aura HD STB to Stalker Middleware. One sees data exchange between the Aura HD STB and Stalker Middleware in the "GET" field under the header "Hypertext Transfer Protocol" (noted in red). The "GET" field shows the portal or domain a device has requested data from. (Ex. 4).

48. The "GET" field in packet 87 (noted in red) shows a data request was made to "stalker_portal." The language "stalker" informs me that the data request was made to Stalker Middleware. Stalker Middleware is downloadable from Infomir's website. (Khan Aff. at 5).

49. The source of the data request in packet 87 was the Aura HD STB because the source IP address was "192.168.12.136," which we have already confirmed is the Aura HD STB's IP address. This information shows us that the Aura HD STB is communicating with "stalker_portal" and corroborates Mr. Vidulich's testimony that his Wireshark capture showed data transfers between the Aura HD STB and a stalker portal. (Vid. Aff. at 5).

50. Further inspection of packet 87's "GET" request reveals that once the Aura HD

STB makes the request on the "stalker_portal," the Aura HD STB is redirected to the domain "online-media.infomir.com." (Ex. 4). This is noted in red at Exhibit 4 underneath the "GET" field where the subfield "Referer" tells us where a data request is redirected, if at all. (Ex. 4). In packet 87's "Referer" field we see the domain "online-media.infomir.com." The presence of "Infomir" in the domain name signifies that this domain belongs to Infomir or an Infomir-related entity and is the source of the data Mr. Vidulich was viewing.

51. This analysis of packet 87's data transfers corroborates Mr. Vidulich's testimony that he witnessed the Aura HD STB connected to the "stalker portal." (Vid. Aff. at 5). Moreover, the Channel One PCAP shows that data transfers are redirected to an Infomir or Infomir-related domain – all while Mr. Vidulich is streaming Russian-language programming.

52. Based on the foregoing analysis and examples, I conclude that the evidence shows that on May 24, 2016 the Aura HD STB communicated with Infomir's Stalker Middleware and an Infomir or Infomir-related domain, which was the source of IPTV streaming video while Mr. Vidulich was watching pirated Russian-language programming. This finding is consistent with the screenshots and statements contained in the Vidulich Affidavit regarding the presence of such data transfers in the Wireshark capture that Mr. Vidulich screenshotted on May 27, 2016.

53. I understand that Infomir argues that it has been disadvantaged by lost evidence. To rebut the allegations that it is pirating video content, Infomir could simply ask its system administrator or lead data technician in charge of its servers to provide Infomir's server log files for May 24, 2016. The server log files for May 24, 2016 would show the MAC addresses and serial numbers for devices communicating with Infomir's servers on May 24, 2016.

54. The Aura HD STB's MAC address and serial number are visible in the Channel One PCAP, for example, in packet 32. Exhibit 5 hereto is a screenshot of packet 32. The MAC

address, "00:1a:79:09:7a," and the serial number, "112012N034702," are highlighted. (Ex. 5).

55. One could then cross reference the Aura HD STB's MAC address and serial number with Infomir's server log files from May 24, 2016 to confirm whether the STB was communicating with Infomir's servers on May 24, 2016. This is a simple process.

C. The Rucinski Report Concedes that the Channel One PCAP Contains Video Data Transfers to the Aura HD STB But Fails to Explain that Infomir is the Source of Video Streaming Transmitted to the Aura HD STB

56. Mr. Rucinski explains that the Channel One PCAP provides deeper explanatory value for the data transfers captured in the Channel One PCAP. (Ruc. Rep. at 9). However, he fails to elaborate what these data transfers would show and where they are coming from. Mr. Rucinski's omission overlooks clear evidence in the Channel One PCAP showing Infomir's servers transmitting video data to the Aura HD STB.

57. One can access video streaming in the Channel One PCAP by analyzing data packets that show the Aura HD STB making requests to a "channel" for streaming. A request made to a "channel" for streaming is indicated by the language "GET /ch/." The screenshot attached hereto as Exhibit 6 shows the language "Get /ch/" in packet 376. Exhibit 6 shows the AURA HD STB making a request to a channel for streaming. (Ex. 6).

58. Digging deeper into packet 376, one can right click on packet 376 to open a menu panel. The screenshot attached hereto as Exhibit 7 shows the menu panel that opens.

59. On the menu panel, clicking "Follow" and then "TCP Stream" opens another window titled "Wireshark – Follow TCP Stream (tcp.stream eq 12) – Channel One Capture" ("TCP Stream Window"). (Ex. 7). A screenshot attached hereto as Exhibit 8 shows the TCP Stream Window.

60. From the TCP Stream Window, we extracted the video streaming evidenced in the

TCP Stream Window. (Ex. 8). The video streaming was saved to a USB drive enclosed to this affidavit. The video data saved to the USB drive is attached hereto as Exhibit 9.

61. The TCP Stream Window also indicates the server source of the video streaming viewed in Exhibit 9. (Ex. 8).

62. Under " Host," we see that the host domain for the video streaming collected in Exhibit 9 is "allfreetv.net." (Ex. 8).

63. We can see that the domain "allfreetv.net" is controlled by Infomir's servers. This is found by conducting a "domain block search" of the domains that Infomir's servers control. A "domain block search" is a search of domains that belong to an organization. The domain block search for Infomir shows the domains that Infomir's servers control.

64. The domain block search conducted for Infomir is accessible at the following webpage: http://ipv4info.com/domains-in-block/s0ea210/79.142.197.0-79.142.197.255.html.

65. At the webpage http://ipv4info.com/domains-in-block/s0ea210/79.142.197.0-79.142.197.255.html, we can see that the organization for the domains listed is "Infomir." This search result signifies that any domains found on http://ipv4info.com/domains-in-block/s0ea210/79.142.197.0-79.142.197.255.html are controlled by Infomir's servers.

66. Scrolling down to line 63, we see the domain "allfreetv.net" – the host domain listed in the TCP Stream Window. (Ex. 8), I have taken a screenshot of line 63 showing the "allfreetv.net" domain, attached hereto as Exhibit 10. Because "allfreetv.net" is listed in Infomir's domain block search described above, we know that Infomir's servers control the domain "allfreetv.net." (Ex. 10).

67. Therefore, the Aura HD STB was receiving video streaming (Ex. 9) directly from Infomir's servers on May 24, 2016. (Ex. 10).

68. Based on this and google searches of Infomir and data distribution reports from Hurricane Electric (ECF 548-25; 548-27; 663-1), it becomes clear that Infomir controls a massive IPTV streaming operation and that numerous servers are under its control.

69. A Google search reveals that Infomir offers 150 Channels and a "Stalker Club" in Ukraine, indicating that Infomir has massive streaming operations.

70. The Hurricane Electric Reports confirm Infomir's streaming into the United States. (ECF 548-25; 548-27; 663-1). These Reports show that Infomir is streaming content to potentially hundreds of thousands of subscribers in the United States by tapping into a widespread data distribution network facilitated by data centers like Hurricane Electric that have large distribution servers in the United States. (ECF 548-25; 548-27; 663-1).

71. Because the Rucinski Report is silent on the source of the video that Mr. Rucinski concedes that the Channel One PCAP shows and because there is overwhelming evidence that Mr. Vidulich viewed an IPTV stream that is part of a massive illegal IPTV streaming operation, the Rucinski Report's suggestion that Infomir was not the source of video streaming should be rejected.

D. The Vidulich Affidavit's May 27, 2016 Screenshots of the May 24, 2016 Wireshark Capture Accurately Demonstrate the Occurrence of Data Transfers Between the Aura HD STB and Infomir Stalker

72. Mr. Rucinski concludes:

> If Mr. Vidulich was watching a live broadcast of Channel One television programming at the same time that the Channel One Screenshots were taken, indicated as May 27, 2016 in the Channel One Screenshots, then the source of the Channel One television programming that Mr. Vidulich was watching was not being captured by Wireshark as depicted in the Channel One Screenshots. (Ruc. Rep at 3).

73. This conclusion is contradicted by Mr. Vidulich's November 20, 2018 Affidavit in which he explains that when he took the screenshots, he was not generating a new Wireshark

capture or viewing Channel One television broadcasting on May 27, 2016. The May 27, 2016 date of the screenshots taken of the May 24, 2016 Channel One PCAP is correctly identified by Mr. Rucinski as the date such screenshots of the earlier Wireshark capture were taken.

74. To be clear, Mr. Vidulich's May 27, 2016 screenshots were of the Wireshark capture that took place on May 24, 2016. Once a Wireshark capture occurs, the data captured is frozen in time and cannot be subsequently altered. The fact that Mr. Rucinski, myself, and others can open the Channel One PCAP in Wireshark, analyze the data captured on May 24, 2016, and take new screenshots demonstrates this to be the case.

75. Mr. Rucinski effectively concedes the static nature of the Channel One PCAP when he states that "Wireshark…is a software program that allows a user to create a record of data packets transmitted across a computer network by 'capturing' the data packets in a file. Wireshark can also be utilized by a user to subsequently analyze the captured data packets, and such analysis can include identifying the source, destination, and content of the captured data packets." (Ruc. Rep. at 2-3).

76. Therefore, although a screenshot of a Wireshark capture shows only the existence of such a capture without the capabilities of analyzing the data captured, to the extent it shows any data communication in the actual image, a screenshot can – and in this case does – accurately present whether data transfers were occurring and the source and destination of such transfers.

E. The Rucinski Report's Reference to Screenshots of a TeamViewer and Skype Session on May 19, 2016 Have Nothing to Do With a Wireshark Capture on May 24, 2016 and Do Not Suggest that Data Was Lost or Spoliated or that Mr. Vidulich's Observations Were Inaccurate

77. Mr. Rucinski reference to screenshots Bates stamped CHANNELONE002592, CHANNELONE002595-2597, and CHANNELONE002599-2602 ("TeamViewer Screenshots") as screenshots that show that the TeamViewer program was running as well as Skype when the

screenshots were taken (Ruc. Rep. at 16) have nothing to do with the loss or spoliation of evidence and do not show that Mr. Vidulich's observations were inaccurate.

78. Mr. Vidulich explains by affidavit dated November 20, 2018 that the TeamViewer Screenshots were not screenshots of his Wireshark capture on May 24, 2016. The TeamViewer Screenshots were screenshots from his instructional session with myself and my technical support team on May 19, 2016. As shown in the TeamViewer Screenshots, I was using Skype, username "tirastel," and TeamViewer to instruct Mr. Vidulich on how to use the Wireshark program to capture data transfers of an STB and how to interpret and analyze such data transfers.

79. For example, the TeamViewer Screenshot attached as Exhibit 1 to Mr. Vidulich's November 20, 2018 affidavit shows that the date the image produced at CHANNELONE002592 was taken was May 19, 2016 according the native file's properties.

80. The screenshots used in the Vidulich Affidavit attached thereto as Exhibits 14 and 16, in contrast, show that neither TeamViewer nor Skype were running at the time Mr. Vidulich took the screenshot. The date shown on the computer screen for Exhibit 14 and 16 screenshots was May 27, 2016 – eight (8) days after the instructional screenshots reflected in the TeamViewer Screenshots.

81. Therefore, the May 27, 2016 screenshots of Mr. Vidulich's May 24, 2016 Wireshark capture have nothing to do with the TeamViewer Screenshots and nothing to do with the Channel One PCAP.

82. Moreover, Mr. Rucinski fails to explain the significance of these screenshots with respect to data allegedly being lost or spoliated. (*Id.* at 16-17). Instead, Mr. Rucinski simply notes that these screenshots show that there was an active skype call with "tirastel" and the program, TeamViewer, was running. (*Id.*) Mr. Rucinski goes on to explain that TeamViewer is a remote

desktop access and support program allowing third parties to take control of another computer. (*Id.* at 17).

83. While Mr. Rucinski's explanation of TeamViewer is accurate, he fails to show how the use of Skype and TeamViewer relates to the loss or spoliation of data from the Channel One PCAP. Had he done so, however, such an argument would have been without merit because Skype and TeamViewer cannot cause the loss or spoliation of data from a Wireshark capture.

84. Even if TeamViewer or Skype had been running during a Wireshark capture, the person communicating with the laptop user through these programs could not alter or manipulate the data capture that occurred on Wireshark. Such data capture occurs in real time and cannot be impacted by TeamViewer or Skype because TeamViewer only allows one to remotely control the interface of another's computer and Skype is instant messaging or real-time audio/video chatting.

85. As such, TeamViewer or Skype cannot manipulate data coming in and out of an STB. Therefore, even if these programs had been running (which they were not), the Wireshark capture from May 24, 2016 is a true and accurate capture of the data transfers that went into and out of the Aura HD STB on that date.

86. In addition, even if TeamViewer and Skype had been running during the Wireshark capture, to the extent that data transfers between the outside computers had been shown in the Wireshark capture, such data transfers would have been shown as separate and distinct from the Aura HD STB data transfers in the ".pcap" file. This is confirmed by my explanation above showing how one can isolate Aura HD STB data transfers and data packets from transfers with other sources and destinations. Being able to control for data packets only showing Aura HD STB transfers demonstrates that the simultaneous running of Team Viewer or Skype would not block or manipulate such data transfers.

87. Based on the foregoing, Mr. Rucinski's reference to the TeamViewer Screenshots is immaterial and irrelevant to any question of data spoliation or the accuracy of the Vidulich Affidavit.

II. The Rucinski Report Should be Rejected Because Rucinski Never Plugged In His STB to Determine Whether Infomir Was Streaming: The Evidence Shows That Infomir Manufactures and Sells STBs with Software to Stream Illegal IPTV

A. The Rucinski Report Should be Rejected Because He Never Attempted to Stream IPTV From His STB or He Did Not Disclose the Results of Such Tests

88. Although Mr. Rucinski reports that he was given an AURA HD International set-top-box serial number 112012N034374 to prepare an expert report, his report does not show the results of his testing of the AURA HD box. A copy of the firmware in Mr. Rucinski's possession (installed in the AURA HD STB) would likely show that the AURA firmware is pre-loaded to point the consumer directly to Infomir-controlled portals to provide pirated Russian-language programming. Because Mr. Rucinski has either failed to test the box in his possession or, in the alternative, has concealed the results of any such tests, his report is flawed and should be stricken.

89. Had Mr. Rucinski tested the box, loaded with the AURA firmware available at Infomir's website, it would have led to results similar to that experienced by Mr. Vidulich. Because Mr. Rucinski failed to test the STB and report the results of his test, Mr. Rucinski cannot show any prejudice to Infomir from lost or spoliated evidence.

B. MAG STBs Show that Infomir Manufactures and Sells Set-Top Boxes

90. Exhibits 1 and 2 to the Khan Affidavit are screenshots of the Vendor listing in the Device Information screen for two STBs, MAG254 and MAG256. The vendors listed are "Teletec" for the MAG254 STB and "Infomir" for the MAG256 STB.

91. Reviewing the Teletec website at http://teletec.com.ua/en/, I can see that Teletec has the same address as Infomir JSC, the Ukrainian branch of Infomir, and is a partner of Teletec.

Based on this, I conclude that the manufacturer and seller of the MAG254 STB is Infomir and the manufacturer and seller of the MAG256 STB is also Infomir or an entity that has the same address as Infomir.

C. Software Development Kits from Infomir's Website Contain Default Programming to Infomir Stalker

92. Infomir's website at the webpage http://soft.infomir.com/ provides for the download of Infomir's AURA firmware onto various STB models. (Khan Aff. at 5). From personal knowledge, I know that firmware is software that provides the low-level control for the STB hardware and performs all control and data manipulation functions like a user interface and navigation. Firmware is also what communicates with middleware, software that is programmed into data centers and servers to reach devices like STBs with firmware on them.

93. At the bottom of http://soft.infomir.com/, I see a link to "SDK STB." From personal knowledge, I know that "SDK" stands for "Software Development Kit." Next to "SDK STB," I see the explanatory text "Utilities for building firmware." From this, I conclude that the "SDK STB" link provides mechanisms for individuals to build and manipulate the AURA firmware to program onto STBs. (Khan Aff. Ex. 14) (sample pages from the "SDK STB").

94. Reviewing these pages, I see that the default programming in the SDK for the AURA firmware is source code connecting the STB to Stalker Middleware. CHANNELONE003385, for example, contains the text "Infomir Stalker." (Khan Aff. Ex. 14). This text appears as an icon in the user interface when one connects a STB programmed with this AURA software.

95. CHANNELONE003482-003497 contains the text "http://echo-01.infomir.com/," "http://echo-02.infomir.com/," "http://echo-03.infomir.com/," and "http://echo-04.infomir.com/." (Khan Aff. Ex. 14). "Echo" is language related to internet connectivity testing. This means that an

STB programmed with this AURA firmware will use the "echo" command to verify a connection with a server. Here, the default server in the SDK's AURA Firmware is Infomir or an Infomir-related server as indicated by ".infomir.com" following the "echo" connection test in the AURA firmware source code. (Khan Aff. Ex. 14).

96. CHANNELONE003663 shows that default programming for image updates in the AURA firmware runs through Infomir or an Infomir-related server. (Khan Aff. Ex. 14). From personal knowledge, image updates refer to updates to images things likes icons that appear in the STB's user interface. The text "aurahd.infomir.ua/imageupdate" appearing in the source code is the default URL where a STB with this firmware programming would get its image updates. The ".infomir.ua" language in the AURA firmware source code indicates that Infomir or an Infomir-related entity is the default server for image updates to the firmware.

97. The Rucinski Report is silent on the issue of whether the STB Mr. Rucinski examined for his report was programmed with the AURA firmware to have Infomir as the default resource for illegal IPTV streaming, consistent with Infomir's SDK. The foregoing analysis however suggests that the STB Mr. Rucinski examined was pre-programmed to connect to Infomir-sourced illegal pirated content. As explained below, had Mr. Rucinski run the appropriate test, it would have confirmed Mr. Vidulich's experience of viewing pirated programming streamed by Infomir.

III. Our Independent Wireshark Capture of an Infomir MAG STB Confirms that Video Content is Routed Through Infomir STBs Confirming the Flawed Methodology of the Rucinski Report

98. In late October through early November 2018, my technical team at Kartina ran an independent MAG STB investigation.

99. We purchased an original Infomir MAG351 STB from Amazon on October 30,

2018 that was preloaded with AURA firmware. Attached hereto as Exhibit 11 is a copy of the order confirmation for the purchase of the original Infomir MAG351 STB from Amazon.

100. Upon arrival, a photo of the a label on the packaging of the original Infomir MAG351 STB was taken. A copy of this photo is attached hereto as Exhibit 12. The label has "Infomir" on it alongside the Infomir logo.

101. A photo was also taken of a pamphlet that came with the packaging of the original Infomir MAG351 STB. A copy of this photo is attached hereto as Exhibit 13. Under "Product Information," one sees "Infomir" alongside the Infomir logo.

102. On November 2, 2018, we set up the original Infomir MAG351 STB and connected it to the internet and a display screen. Once configured, a photo of the "Device Info" screen was taken. A copy of this photo is attached hereto as Exhibit 14. Like the photo of the MAG256 "Device Info" screen attached to the Khan Affidavit, the original Infomir MAG351 STB screen also shows "Infomir" as the "Vendor." (Ex. 14; Khan Aff. at 2).

103. We then ran a Wireshark capture of the original Infomir MAG351 STB while streaming pirated Russian language programming. The ".pcap" file that was generated by the Wireshark capture was uploaded onto the same USB drive that contains Exhibit 9. The file is attached hereto as Exhibit 15. The file can be viewed using Wireshark.

104. The Wireshark capture shows video data being routed to the original Infomir MAG351 STB through passwords purchased for the streaming portals "Ozo" and "Sovok." (Ex. 15). The URL for "Ozo" is http://portal.ozo.tv/. The URL for "Sovok" is http://aura.sovok.tv/.

105. One can view this video data by clicking "Export Objects" under the "File' tab of the Wireshark capture file. (Ex. 15). From there, one can click "HTTP" to narrow the files being exported to only HTTP data files. (Ex. 15).

106. We saved these HTTP communications into a folder on a computer hard drive and further refined therein by deleting any files that did not contain video data. "TS" files contain video data. So, any files that were not "TS" files were deleted, leaving the "TS" video files.

107. The "TS" files were then saved to the same USB drive where Exhibits 9 and 15 were saved. The "TS" files are attached hereto as Exhibit 16.

108. The video files saved in Exhibit 16 are video content that was being routed to the original Infomir MAG351 STB and projected onto the display screen on November 2, 2018. (Ex. 16). Opening one of the Exhibit 11 video files with a basic media player like Windows Media Player, one can see the actual video streaming being transmitted to the STB. (Ex. 16).

109. The videos contain branding and logos for Channel One that are displayed on the top right hand corner but we did not purchase Channel One streaming content from Channel One. (Ex. 16).

110. Because Mr. Rucinski presumably could have run the same tests with the same result showing Channel One content being streamed through Infomir's STBs, Mr. Rucinski's conclusions are flawed and should be rejected.

111. Based on the foregoing. I conclude that the Rucinski Report is unreliable, incomplete and flawed. The evidence I have reviewed shows that today Infomir continues to sell MAG STB's that enable users to stream unauthorized IPTV programming and engages in providing unauthorized IPTV pirated content to users in the United States.

Dated: Wiesbaden, Germany
December 7th, 2018

DMITRI DIETRICH